Performance Evaluation of Secure OLSR under Link Spoofing Attack

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted by

Aditi

(801433002)

Under the Supervision of

Dr. Ashutosh Mishra

Assistant Professor

(CSED)

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

June 2016

Certificate

I hereby certify that the work which is being presented in the thesis entitled, "*Performance Evaluation Of Secure OLSR Under Link Spoofing Attack*", in partial fulfilment of the requirements for the award of degree of Master of Engineering in Information Security in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Ashutosh Mishra and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Aditi

(Aditi)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Ashutosh Mishra)
Assistant Professor,
Computer Science and Engineering Department
Thapar University

Countersigned by

(Dr. Maninder Singh)
Head,CSED
Thapar University
Patiala

(Dr. S.S. Bhatia)
Dean (Academic Affairs)
Thapar University
Patiala

Certificate

I hereby certify that the work which is being presented in the thesis entitled, "*Performance Evaluation Of Secure OLSR Under Link Spoofing Attack*", in partial fulfilment of the requirements for the award of degree of Master of Engineering in Information Security in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Ashutosh Mishra and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Aditi)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Ashutosh Mishra)
Assistant Professor,
Computer Science and Engineering Department
Thapar University

Countersigned by

(Dr. Maninder Singh)
Head,CSED
Thapar University
Patiala

(**Dr. S.S. Bhatia**)
Dean (Academic Affairs)
Thapar University
Patiala

Acknowledgement

No volume of words is enough to express my gratitude towards my guide, **Dr. Ashutosh Mishra**, Assistant Professor, Computer Science and Engineering Department, Thapar University, who has been very concerned and has supervised the work presented in this thesis report. He has helped me to explore this vast field in an organized manner and provided me with all the ideas on how to work towards a research oriented venture.

I am also thankful to **Dr. Maninder Singh**, Head of Department, CSED and **Mrs Jhilik Bhattacharya**, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my **parents**, **friends** and the **Almighty** for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.

Aditi

Abstract

Mobile ad hoc network (MANET) is a dynamic in nature which is constantly prone to many severe attacks. It has a many unique features unlike conventional network. It is a node resource constraint and self-constructed network. In this thesis, we summarized basically security vulnerabilities in the optimized link state routing protocol (OLSR). OLSR is mostly primarily for dense networks. The paramount feature of OLSR is multipoint relay nodes. In our work, we suggested a prototype to defend against link spoofing attack. Our main technique is based on interchanging control packets by 2-hop neighbors. The major ease of our approach is that it offers protection against link spoofing attack without having knowledge of complete scenario. In our scenario we do not need particular hardware like Global Positioning System (GPS). Secure-OLSR is implemented on network simulator. Our simulation analysis indicates that proposed algorithm is good enough to detect presence of malicious node under link spoofing attack as compared to current version of OLSR. Our approach have higher packet delivery ratio, and throughput.

Index Terms—MANET, OLSR, routing, vulnerabilities

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 MANET

In recent years lot of research is being done on different aspects of wireless networks. Mobile ad hoc Network [MANET] is the kind of the wireless network.

Mobile ad hoc Network are networks which have movable nodes with no central administration. They communicate via radio waves. MANETS follow multi-hop approach. In this approach if nodes are not in transmission range of each other for communication then intermediate nodes help to forward the packets to other ad hoc network [1]. For example in Fig 1.1 shows the multi hop approach in which node S and node D are not in transmission range or are in different networks however, intermediate nodes will help to forward the packet i.e. node F will forward the packet and act as router.

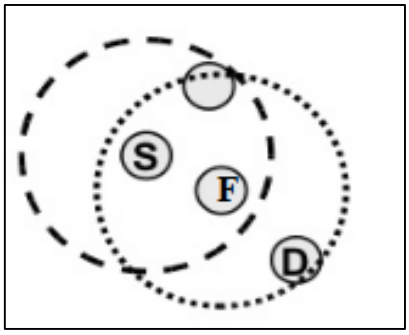

Fig 1.1 Multi-hop approach in MANETS

MANETS have temporary infrastructure or we can say that it has no fixed infrastructure. It changes frequently. Therefore mobility causes route changes. They periodically update the network with the fresh information within some interval of time. MANETS are fully distributed. MANET is in trend because of its unique feature like low bandwidth and power consumption [2]. MANET have dynamic topology in which nodes are free to act as router or host to disseminate information into the network. A MANET is depicted in Fig.1.3 and infrastructure network is depicted in Fig 1.4.

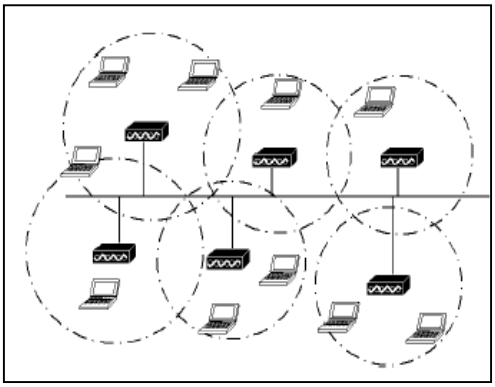

Fig.1.2 Infrastructure Network

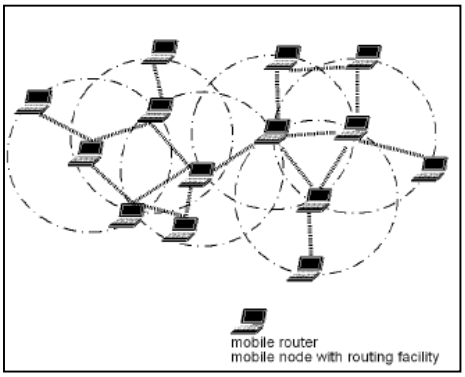

Fig.1.3 Mobile ad hoc Network

1.1.1 Characteristics of MANETs

- Fully distributed: These network does not have any central entity for controlling the network. Only nodes should cooperate with each other and load of the network is distributed among nodes.
- Dynamic topology: In MANETs nodes are open to progress anywhere in the network with varying speed. Because of the movement of nodes, the topology of network changes regularly and at arbitrary time [3].
- Multi-hop routing: These networks follow this approach where nodes are not in domain of each-other. In this routing, the intervening nodes forward the packet.
- Limited bandwidth: Wireless network have lower bandwidth capacity than wired network.
- Routing updates: MANETS are have the latest information about the links and nodes [2].

1.1.2 Advantages of MANETs

- It is self-configuring network without any central network administrator.
- The network is flexible which can be deployed at any place and time.
- It is more scalable than any wired network.
- The nodes in the MANETS play very crucial role. They do not require any hardware or software for communication among themselves [3].

1.1.3 Disadvantages of MANETs

- It is difficult to detect malicious node in the network because of volatile network topology.
- They have limited resources
- Nodes are dependent on batteries for power consumption Therefore operations are more restrictive.
- It does not guarantee if the nodes in the network are polished or not [2].

1.1.4 Application of MANETs

- Military or police exercises.
- Disaster relief operations.
- Mine cite operations.
- Urgent Business meetings [4].

1.2 Routing Protocols

In MANETs routing protocol plays a very important role for maintaining, creating and recalculating the routes which are flexible, durable, adaptive and more secure. To run smoothly Ad Hoc network requires quick, secure and adaptive routing protocol that at the same time does not consume too much of the already scarce wireless bandwidth and provide the secure communication. MANET routing protocol is categorized as proactive and reactive routing protocols. Reactive is a search process for a route from source to destination node only when required [4]. No periodic exchange of message takes place until it is required. Some of the protocols which comes in this category are Dynamic Source Routing (DSR), Ad hoc On-Demand Distance Vector Routing AODV [2]. On other hand proactive routing protocol maintains routing table for each node from source to destination. It has continuous exchange of messages. Protocols which belong to this category are Destination Sequence Distance Vector (DSDV) [3] and Optimized Link State Routing (OLSR) [3] protocols. The classification of the protocols

are as based on how they collect the information about the network [5] and shown in Fig 1.4.

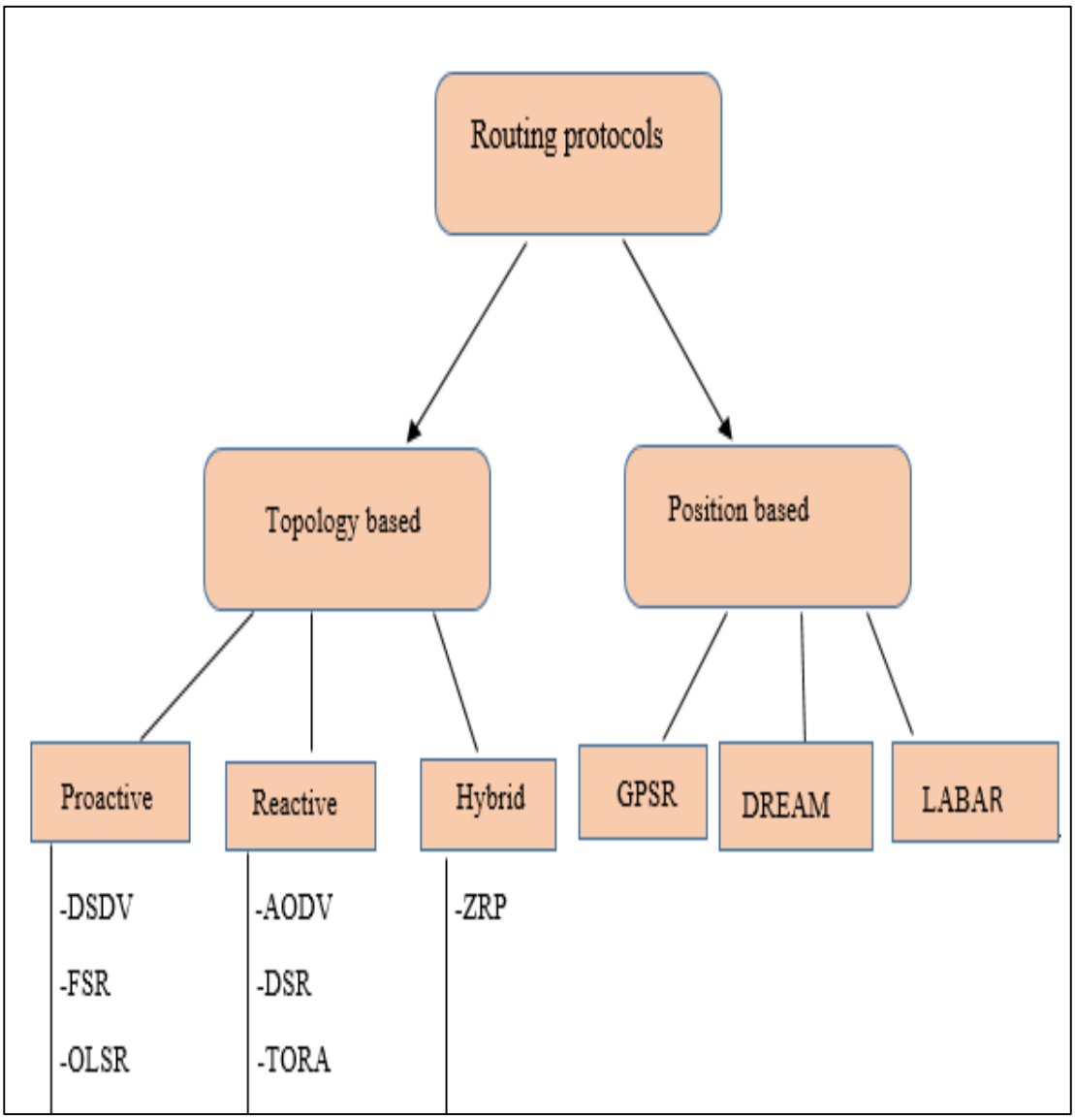

Figure 1.4 Classification of routing protocols

1.3 Topology Based

It is based on link's information within the network for sending data packets from source to destination. It has all the information about the links i.e. whether a symmetric link exist or asymmetric link [6].

1.4 Reactive Routing

They are also known as Source-Initiated-On demand routing. This type of routing calculates route only on demand of source node. In this routing for finding the route from origin to destination end is the route discovery process. All the possible route permutations are done to find the shortest and secure route from source to destination. After the establishment of routes, its maintenance is done by route maintenance procedure [7] [8].

1.4.1 Ad hoc On Demand Distance Vector Routing Protocol (AODV)

It is pure on demand route acquisition system. The participating mobile nodes in the network obtain routes quickly and updates other nodes also. The nodes who are not participating in the network does not participates in routing table exchange. The path discovery process is done for locating the others node by broadcasting Route Request (RREQ) packets to other neighbors [9] and is shown in Fig 1.5. The operation of AODV is loop free and maintains the most-latest information. Every node has its own sequence number and broadcast ID.

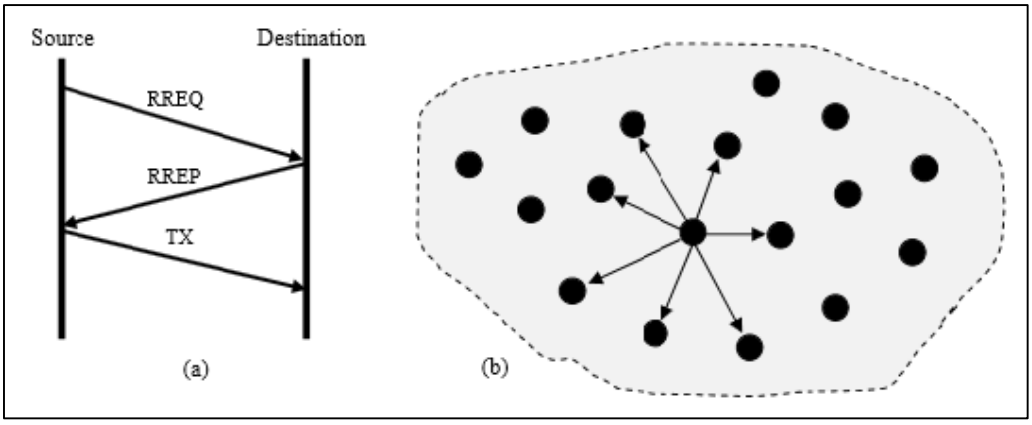

Figure 1.5 Route request for AODV

The predominant objective of the AODV is

- Discovery packets are to be broadcasted only when needed.

- Maintenance of the topology.

- Dissemination of the information about the changes in the network occurred.

1.4.2 Dynamic Source Routing Protocol (DSR)

This protocol is inspired from link state routing algorithm. The main catch of the DSR is that each node stores the hop sequence to the destination [10]. They regularly advertise the control packets which is shown in Fig 1.6. It follows two mechanism:-

- Route discovery

- Route maintenance

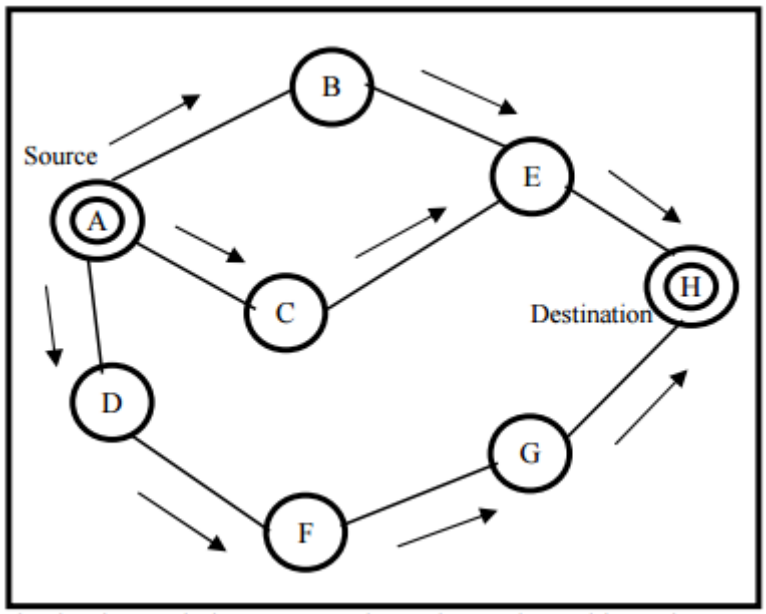

Figure 1.6 Working of DSR

1.4.3 Temporally Ordered Routing Algorithm (TORA)

It is on demand routing protocol based on link reversal algorithm. The main purpose of the protocol is to limit control message propagation. Tora performs three functions mainly creation of route, maintenance of route to destination and keep up to date which route is invalid. It takes help of Directed Acyclic Graph (DAG) for building route to destination. This protocol uses three types of messages: QRY message (route creation), UDP message (route maintenance), CLR message (Erasing routes) [11].

1.5 Proactive Routing

Proactive routing protocol maintains routing table for each node from source to destination. It has continuous exchange of message. Protocols which belong to this category are Destination Sequence Distance Vector (DSDV) [3] and Optimized Link State Routing (OLSR) [3] protocols.

1.5.1 Optimized Link State Routing Protocol (OLSR)

The proactive [table-driven] routing protocol, OLSR is the latest effort to reduce the overhead of the DSDV protocol. It is designed for mobile ad hoc network. OLSR provides the benefit of optimal routes to the network when needed, due to its proactive nature. It uses hop-by-hop approach and flooding mechanism [1] [3]. It works in distributed manner. The objective of this protocol is to avoid unnecessary transmission of control packets. Each node decide which of its neighbors can flood control packets, these nodes are known as MPR nodes. Only "*multi point relay*" (MPR) are privileged to forward, generate and retransmit the control packets [3].The updates are sent regularly. It does not need orderly delivery, since sequence numbers (MSN) are used to prevent extinct information from being misunderstood. It is appropriate for large and thick networks. The primary concept of the protocol is MPR nodes. All node in the mesh elects a group of 1-hop neighbor nodes as "multipoint relays", which diffuse the topology information into the entire network. They help in limiting the traffic [3] [5] [6]. Neighbors which are not "MPR" (N) operate uniquely control packets of N node, but the forwardness of the control packets is not there. "MPR" (N) nodes are elected in this way that they are capable to cover all 2-hop neighbors of the network. In Fig 1.7 (a) regular flooding does 24 retransmission for diffusing message to 3-hop neighbor and in Fig 1.7 (b) MPR nodes reduces the number of transmissions to 11.

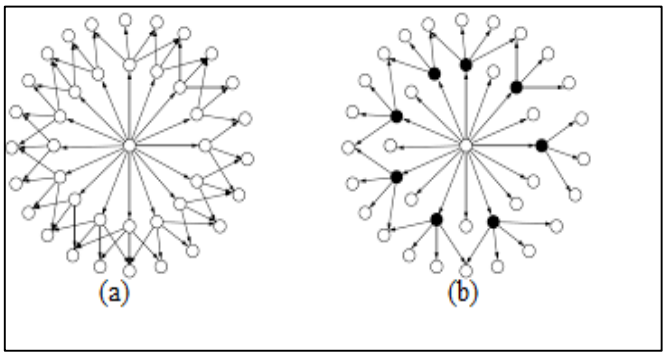

Figure 1.7 [5] Optimized Link State Routing Protocol

1.5.2 Working of OLSR

OLSR consists of two kinds of routing packets, namely HELLO packet and Topology control packet (TC).

Hello packet*:* All node utilize their HELLO messages to get aware of its MPR set and link sensing. Each nodes regularly declare HELLO messages to the set of 1-hop neighbor [12]. They are not forwarded further. The received HELLO message gives the information of 2-hop neighbourhood and ideal MPR set. A "Sequence number" (MSN) are related with the MPR set, which is increased by one. In Fig 1.8. Node A advertises the hello packet to its 1-hop neighbor and update its routing table with latest information by HELLO: NBR (A) = {B,E,F,C}.

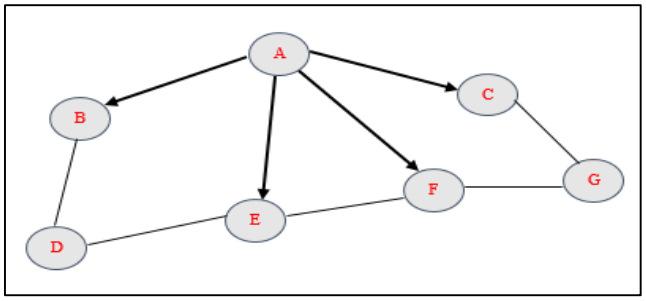

Figure 1.8 Broadcasting of Hello Packet

TC packet: Nodes which are selected as MPR nodes, periodically diffuses TC message in the network having the list of MPR selector. This packet is used for routing table calculation. Only MPR nodes are privileged to forward TC packet [13]. In the following figure the node E generates the TC message and broadcasting in the network. The green arrow in the Fig 1.9 indicates the broadcasting of topology control packet. The TC message of the node E is depicted as MS (E) = {D, B F}. Further node B and C forwards the E' TC message.

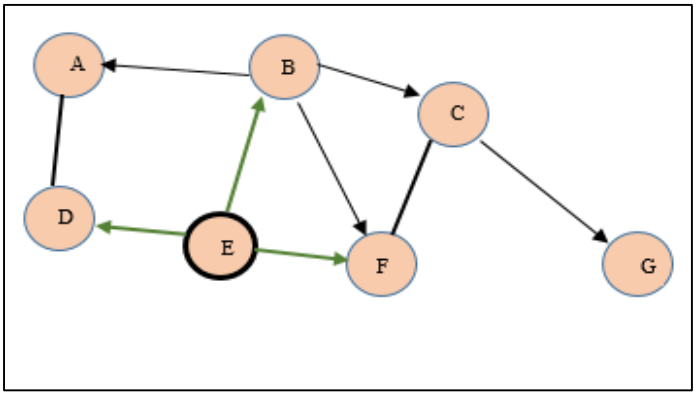

Figure 1.9 Broadcasting of TC message

MPR selection

Each node selects its MPR nodes independently from the subset of 1-hop neighbour [14]. They must be capable of covering the 2-hop neighbors. MPR set is recalculated when a change in the 1-hop or 2-hop neighborhood is detected. Minimum set of MPR nodes results to the more optimal protocol. Let us take a scenario in which we have different nodes in the topology in Fig 1.10.

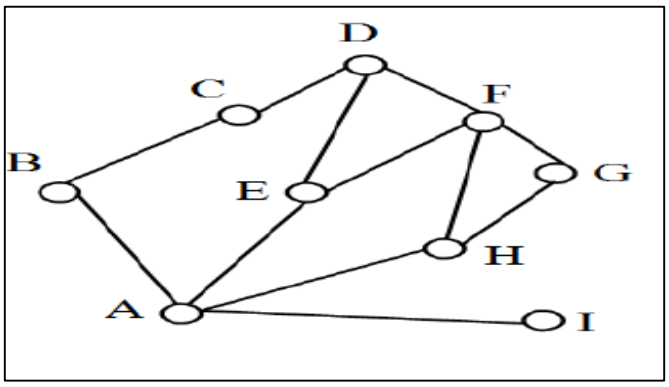

Fig 1.10 MPR Selection Process

In the MPR selection procedure for node A, it broadcast hello message packet to its 1-hop neighbor {E, H, I, B} and its 2-hop neigbor are {F, G, D, C}. The nodes express their willingness by hello packet. Node A will select E as its MPR because it is able to cover all the 2-hop neighbors.

1.5.3 Destination-Sequenced Distance Vector Routing (DSDV)

It is the table driven routing protocol. The ground of DSDV is Bellman Ford algorithm. The vital objective of the DSDV is that it overcomes routing loop problem. This protocol tries to deliver its packet by the shortest route using Dijkstra's shortest path algorithm. It keeps the routing table of each node up to date and assemble the information of network topology. The routing table have information like destination address, number of hops, destination sequence number. This algorithm have count to infinity problem [15].

1.5.4 Fisheye State Routing (FSR)

It is one of the proactive routing protocol. It is established from link state routing. The chief goal of this routing protocol is to minimize the routing update overhead in big networks. Its functionality is similar to other protocols but it uses different exchange periods in routing table. FSR uses the concept of scopes for sending the link state

updates which is given in Fig 1.11. It sends in the form of ($2^{k-1}T$), where k is the hop distance and T is the transmission period of link updates. The distance is directly proportional to exchange frequency [16].

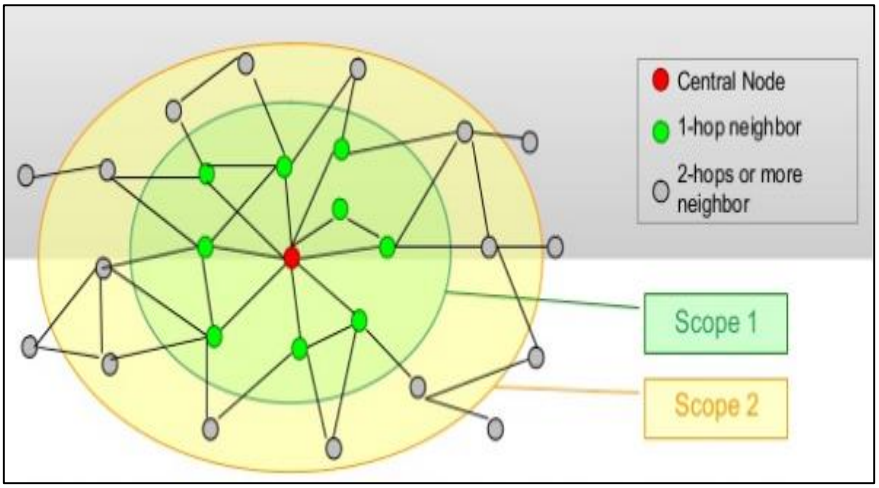

Fig 1.11 Model of Fisheye State Routing

The main drawback of this prototype is that routing table grows linearly large and for remote destination it can't upgrade the routes.

1.6 Hybrid Routing

This routing is the combination of proactive and reactive routing protocol. Its main function is to gather routing information and maintain it when the network topology changes. The procedure followed by Hybrid routing is that a set of nodes accumulate in their different zones. In these zones different proactive approach is applied. The route discovery and route maintenance are done from one zone to other different zone. The familiar hybrid routing protocols are Zone Routing Protocol (ZRP) [17].

1.7 Attacks on OLSR

OLSR protocol is vulnerable to different attacks which results into disruption of routing operations and many kind of Dos attacks induce false message in the network for disrupting the

1. Link Spoofing Attack: This attack is done by malicious node for recording, controlling, modifying, dropping or withholding the routing traffic. The selfish node advertise fake link with other neighbor nodes along with its HELLO packet and TC packet. It can be held in many ways either by flooding false

information of non-existing node in the network or by inserting fake link in the network, which will result into an inaccurate routing traffic or forcing victim node to appoint malicious node as MPR [9] This enforces victim node to appoint selfish node as its multipoint relay, hence selfish node can distort data or traffic and can perform miscellaneous variety of Denial of Service (Dos) attacks [4]. Fig 1.12 depicts an attack of link spoofing where M1 is a malicious node and T is target node, which is the TC source node.

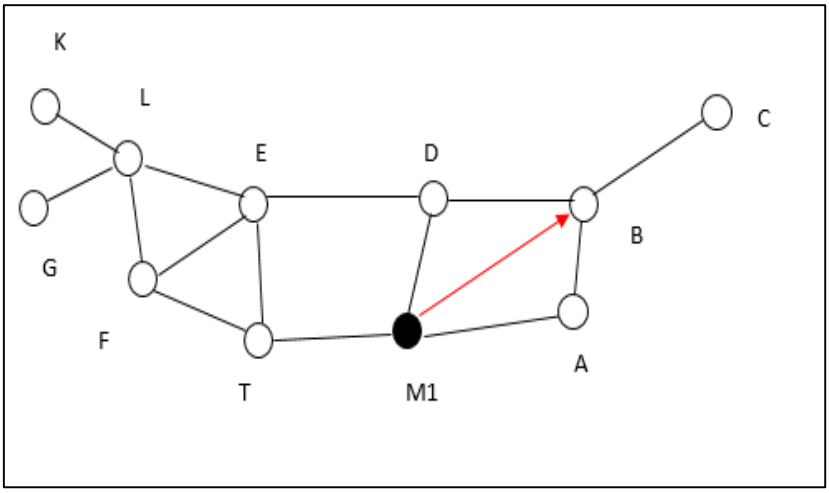

Fig 1.12 Model of Link spoofing Attack

2. Black Hole Attack: The intruder enters the network and sends false information about availability of bogus routes to neighbor nodes. It state that it has the optimal path to the destination node and black hole model is shown in Fig 1.13. For that reason nodes advertise all the data packets to the malicious node, which does not relay packets further and absorb the network resources [5] [18].

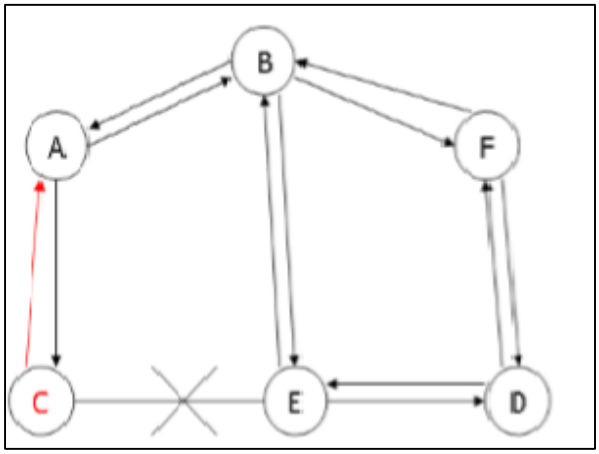

Fig 1.13 Model of Black Hole Attack

3. Wormhole Attack: It is one of the tunnelling attacks in MANETS. The malicious nodes in the grid are referred as worms. It consists of a pair of colluding attackers to create a tunnel with each other and attract maximum traffic towards them. They circulate in the network freely without any knowledge of any node and act as immediate neighbors. The wormhole attacker aims of recording packet of one network and replay them to another network. The model is given below in Fig 1.14.The attacker can easily route and manipulate packets [5] [6].

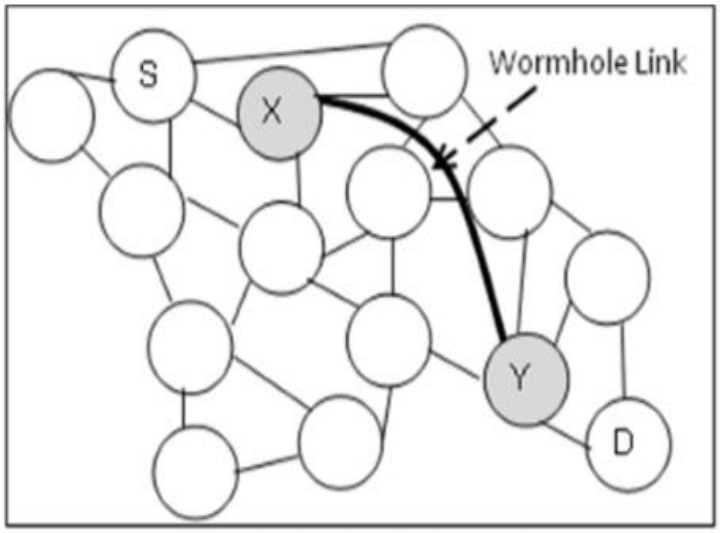

Figure 1.14 Model of Wormhole Attack

4. Node Isolation Attack: It is one of the kind of denial-service-attack (DOS) attack which is done by mischievous node in opposition to OLSR protocol .The isolation of a victim node from exchanging with other neighbor nodes in the network is defined as node isolation attack. This action enables a victim node from accepting data packets [19]. This Fig 1.16 tell us the scenario of the node isolation attack. Node B is the attacker and targeting the victim A. It sends hello message to A and containing the wrong information having a non-existent node in the network such as {A, G, E, Y, F}. So this hello message will force other nodes to select it as a MPR. Then the attacker node can easily manipulate the data packets.

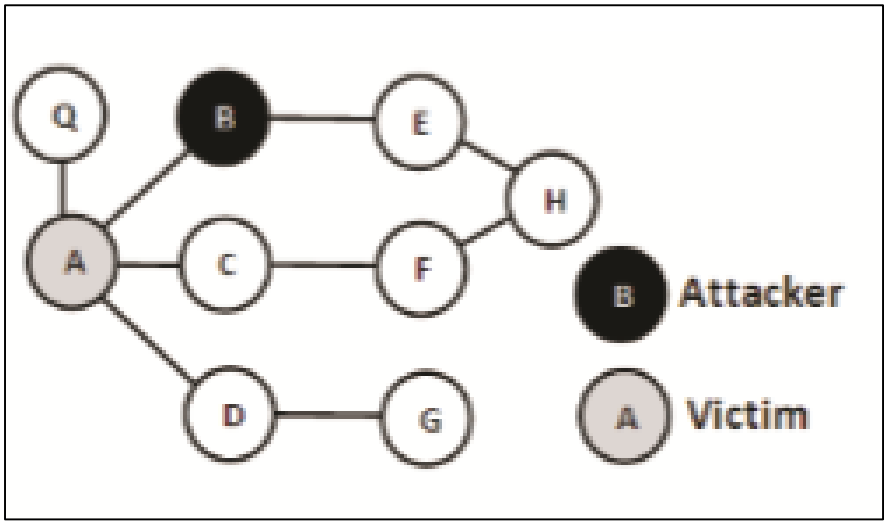

Figure 1.15 Node Isolation Attack

5. Packet Drop Attack: In this attacker targets the *willingness* field which is responsible for carrying traffic to other nodes. The dropper node maintain its field to WILL_ALWAYS and forces for its selection as MPR. The dropper node gets privileged to modify the packets routed through it [20].

6. Grey Hole Attack: It is attack, where attacker behaves normally for some interval of time and drop packet for certain time. This behaviour keep the attacker node at safe side. It is the addition to black hole attack. The grey hole targets three type of attacks. Firstly the node may drop resources for certain interval of time and forwards the rest of packets. Secondly it acts as malicious node only for certain period of time [21].

Kannhavong *et al*. [22] have designed secured routing mechanism based on switching acknowledgement betwixt 2-hop neighbors. The authors have designed this protocol to eliminate vulnerability of the current OLSR and provide protection against sophisticated attacks like link spoofing attack. This algorithm helps to detect the unreliable link in the network. In this approach two elements are added respectively (ACKtc) and trust table along with HELLO packet. In this author have assumed that authentication method is exercised because for the discovery of the original start of every packet which will block selfish node from generating false Acknowledgement (ACK).

Daniele *et al*. [23] has deployed the digital signature mechanism for routing of the message in the network. It is based on authentication checks of information injected into the network.

Soufine *et al*. [24] addressed the problem of cooperative black hole attack. The main purpose of this attack is exploiting the functionality of routing protocol for retaining control packets. They proposed an acknowledgement based technique which will make OLSR less vulnerable to such types of attacks. In this scheme the author has introduced two more control packet i.e. 3 hop_ACK and HELLO_rep.

Zhao, Ziming *et al*. [25] proposed a risk aware technique is to cope with the routing attacks. The approach is based on extended Dempster-Shafer mathematical theory of evidence. D-S theory is an invaluable tool for accessing reliability in information systems. They performed a sequence of simulation experiments with proactive MANET routing protocol.

García Villalba, L. Javier, *et al*. [26] focused on securing the OLSR protocol. The mechanism has used digital signature for signing each OLSR control packet for the purpose of authentication. Timestamps are used by the authors to prevent replay attack on OLSR. The main advantage of this scenario is no need of synchronized time. The drawback of the solution is that adds extra overhead to all the OLSR packets.

Balaji S and Thorat [27] proposed a reputation base mechanism. This mechanism secure against DOS attack. The simulation results of the solution show that routing security

mechanism have increased packet delivery ratio, throughput and control overhead. The main advantage is that there is no requirement of high computational complexity. The simulation results are found by Network Simulator (ns-2).

Wang, Maoyu, *et al* [28] author has proposed a response technique for protecting the OLSR protocol from inside intruders. This approach can be applied to only MPR nodes. Intrusion alarm will trigger if any abnormal protocol semantics occurs.

Vidhya, K. Urmila, and M. Mohana Priya [29] investigated various attacks are injected in OLSR. Attackers can easily isolate a node from the network. The proposed an idea to detect whether the node is selfish or not on the basis of trust analysis. The solution entertained by them takes three parameters HOP_Information, 2-hop request and 2-hop reply.

Mulert, and Welch [30] has main focus on the security of MANET. They proposed secure extension of AODV as SAODV, where they have used cryptographic mechanisms to protect the routing control messages.

Jeon, Yuseok, *et al.* [31] has proposed a mechanism, LT-OLSR which advertise hello message to its 2-hop neighbor .The main area of research is link spoofing attack. Their contribution to this paper was that each node will have its own uncontaminated routing table. LT-OLSR tolerates the link spoofing attack.

João P., and Barros [32] has concentrated on OLSR protocol and proposed Cooperative Security Scheme (CSS-OLSR) which reward each node on the basis of their routing information exchange. They has categorized nodes as behaved nodes and strongly damaging behaviour. In CSS-OLSR they had added three parameters likely to be Complete Path message (CPM), Rating table, Warning message.

Ronggong and Peter [33] has designed a new model Robust OLSR (R-OLSR) for military confidential environment and defending the security vulnerabilities of OLSR. They have added new parameters to OLSR and comprehensive neighbourhood trust model.

Anbao, and Zhu [34] have proposed a new design of MPR technology. The prototype is based on node localization. The implementation is done on network simulator. It has reduces the number of routing packets and make usage of its network resources. The simulation results tell us that this algorithm is feasible and is applicable.

Radhika D and Rege [35] have put their efforts in making OLSR, energy efficient. They have done so by making effective neighbor selection. The primary objective of OLSRM is the route selection and route recovery. The model was designed on R software.

Chapter 3

Problem statement and Objectives

3.1 Problem Statement

Mobile ad hoc network has been attracting many good amount of researchers due to its features. It have self-configuring mobile nodes with no central authority. They can create their setup or infrastructure anywhere. It is open media and changes it topology dynamically. Security becomes major issue of concern. Misbehaving nodes can enter the network and will destroy the whole network. There is no good defence mechanism. The attacker can go easily inside the network and can modify the packets. There are different types of misbehaving nodes which have different functionalities as shown in Fig 3.1 below:-

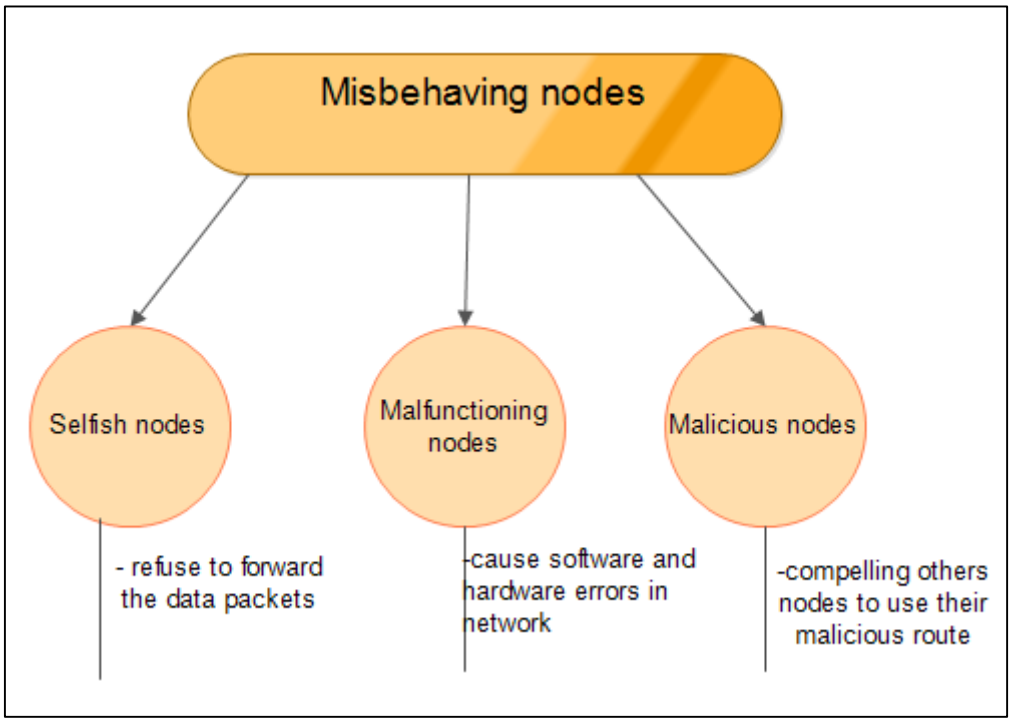

Fig 3.1 Classification of Misbehaving Nodes.

OLSR is the essential routing protocol which is prone to various attacks such as link spoofing, identity spoofing, relay and wormhole attacks. Researchers have provided many security extension to overcome this type of attacks, but they are not successfully yet [5].

The proactive [table-driven] routing protocol designed for mobile ad hoc network, named as OLSR is the optimization of link state algorithm. OLSR provides the benefit of optimal routes to the network when needed, due to its proactive nature. It uses hop-by-hop approach and flooding mechanism [1] [3]. It works in distributed manner.

3.2 Objectives and sub task

In order to achieve a secure protocol we need solitary 2-hop neighbors should generate 2-hop_*ACK* and sends in return to MPR node. In our model we assumed that authentication has been applied to check the validity of the correct origin of every packet to halt from sending false 2-hop_*ACK*. Secondly, our strategy need that each MPR node should be aware of its 2 hop neighbors set in order to distinguish between fake link and genuine link. The 2-hop_*req*, 2-hop_*ACK* and trust table are modified packets which are added with TC message in our scenario for the detection of link spoofing attack. Therefore, by using hop by hop technique we can block any outsider from reaching the network. Thus, applying this mechanism will help to prevent link spoofing attack. The primary objective of this thesis is secure routing in OLSR under link spoofing attack which was achieved by the following manner:

- To analyse, implement and evaluate OLSR protocol.
- Evaluate the behaviour of OLSR under link spoofing attack
- In accordance to know the achievement of the protocol, the throughput under link spoofing attack was analysed.
- Comparative analysis was done between OLSR and S-OLSR under link spoofing attack.
- After that, throughput and packet delivery ratio was observed.
- So, the objective is to ensure security in infrastructure network using secure-OLSR method, and to analyse the throughput as well as packet delivery ratio before and after the implementation of link spoofing attack.

Chapter 4

Proposed Mechanism

4.1 Overview

In this section, we stated the security extension of existing OLSR. Secure-OLSR is used for resisting link spoofing attack. Our mechanism is for checking the presence of malicious node and identifying the fake link in the network. To attain our prototype, we require solitary 2-hop neighbors for generating 2-hop_*ACK* and return to its MPR node. In our model we assumed that authentication has been applied to check the validity of the correct origin of every packet to halt from sending false 2-hop_*ACK*. Secondly, Our strategy requires that every MPR node should be aware of its 2 hop neighbors set orderly to distinguish between fake link and genuine link. The 2-hop_*req*, 2-hop_*ACK* and trust table are modified packets which are added with TC message in our scenario for the detection of link spoofing attack.

- 2-HOP_*req*: The TC source node periodically broadcasts 2-HOP_*req* control packet to its neighbors along with TC packet.
- 2-hop_*ACK*: The 2-hop_*ACK* packet is needed to acknowledge the TC messages which are fully entertained by every node's two-hop neighbors.
- Trust table: Every node maintains its own trust table having initial value to be 0. It is comprises data related to its 2-hop and 1-hop neighbors.

4.2 Proposed Mechanism

The following modifications are made in the original OLSR protocol.

1. When a node receive TC packet from MPR node then they look at their routing table to check if MPR node is its 2-hop neighbour or not. If the source node or MPR node is considered to be its 2-hop neighbour, it sends back 2-hop_ACK to the MPR node else it does not generate any acknowledgement packet.

2. If a correctness of received 2-hop_ACK is verified from 2-hop neighbors, it assumes that link is reliable and truly exists assuming that TC message is successfully received. It sets trust value to be 1.

3. If the selected node is not the 2hop neighbors then no 2-hop_ACK packet is sent hence trust table value of link tuple is 0, node judges that it is forgery link or packets are dropped by selfish node.

4. The nodes in the network gets aware about suspicious link in the topology and avoids that node to be its MPR. Fig 4.1 tells the functioning of algorithm.

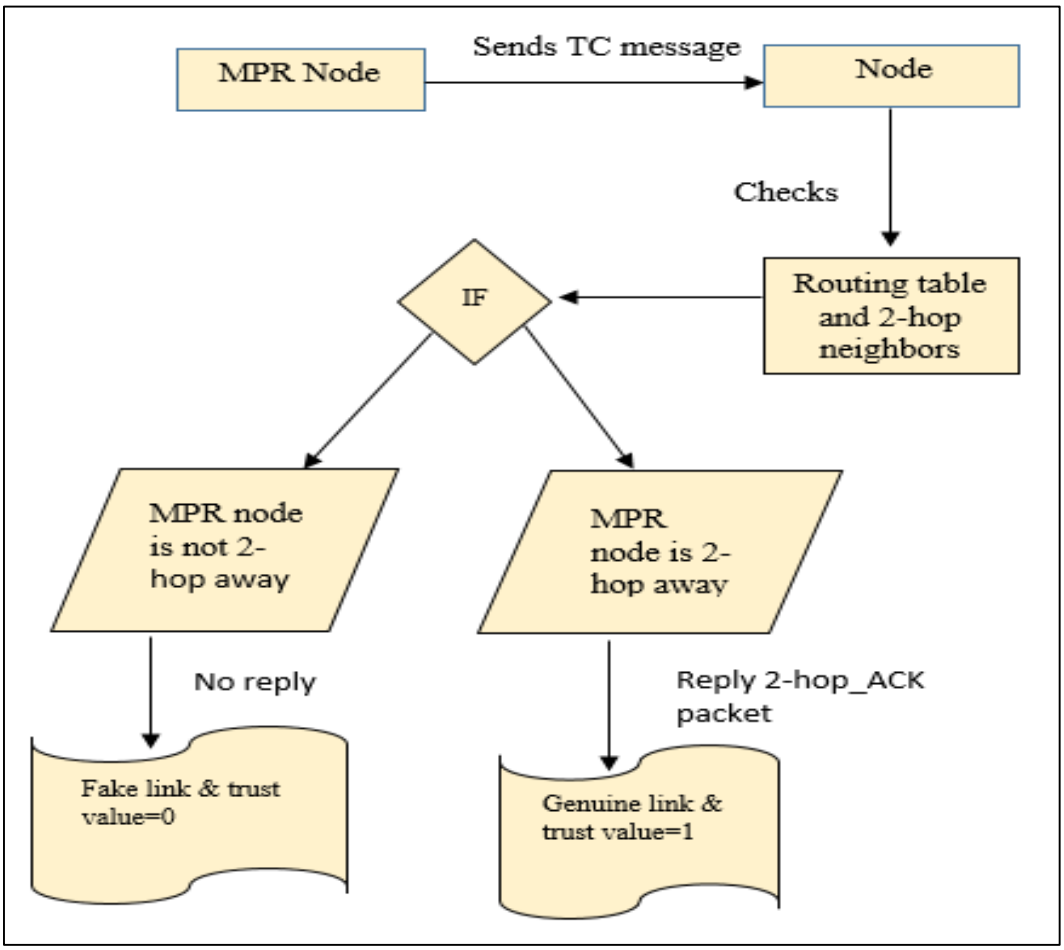

Figure 4.1 Functional Representation of Algorithm

4.3 Explanation

In Fig 4.2 .node T is the MPR node and it is assumed in our scenario that every MPR node knows its 1hop and 2 neighbors list. T sends a 2-HOP_*req* packet along with TC message to its 2-hop neighbors i.e. {G,K,A,E } but malicious node has provided wrong information to node T that F is also its 2-hop neighbour by faking a link with F .Therefore node T will have latest information of its 2-hop neighbors i.e.{G,K,A,E,F}.In Table 4.1 the route table of MPR node T is shown with the latest information. Now malicious node M will force T to route the traffic to F via M which can be very dangerous.

Table 4.1. Routing Table of node T

1-Hop Neighbor	2-Hop Neighbor
L	K
M	E
	A
	G
	F

4.4 Protection Offered

Link spoofing attack can be detected by checking the routing table consisting trust value of a dummy link to be 0 as shown in Table 4.2. The explanation of our mechanism is in Figure. 4 where arrows in blue represent 2-HOP_req packet and arrows in red represent 2-hop*_ACK* packet. In our methodology, T has concluded F is its "2-hop neighbor". But, in fact F is "3-hops" away from T. As our methodology needed all 2-hop neighbors to generate 2-hop*_ACK* packet, F which is T's "3-hop neighbor" will not deliver 2-hop*_ACK* back to node T which will automatically set trust value to 0. Our scheme will bring into knowledge of T that F is not its "2-hop neighbor" and assumes that no link exists between node M and node F. So the presence of fake link is detected to prevent the wormhole and link spoofing attack.

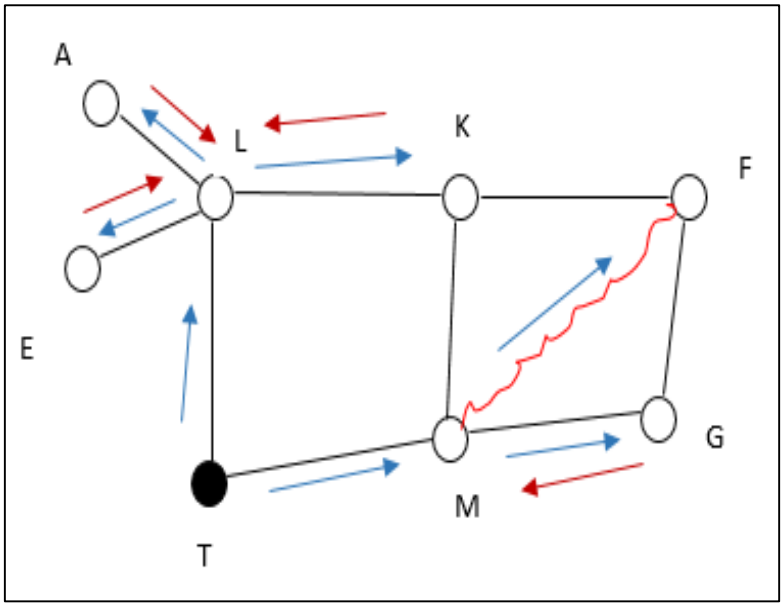

Figure 4.2 Working of Secure-OLSR

Table 4.2 Routing Table with trust value

1-Hop Neighbor	2-Hop Neighbor	Trust Value
L	K	1
M	E	1
	A	1
	G	1
	F	0

Chapter 5

Installation, Simulation and Design

5.1 THE NETWORK SIMULATOR (NS2)

Simulation is the combination of art and science. Simulation process can be defined as the flow process of network entities like nodes packets etc. According to Shannon [36], simulation is "the process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behaviour of the system and or evaluating various strategies for the operation of the system." Simulations are of two type Time-dependent simulation and Non-Time dependent simulation [37].

5.1.1 NS-2 Basic Architecture

NS is made uniquely for computer networks. It helps to predict the performance of the computer network. It was explored at University of California at Berkeley, USA. NS2 is modified from REAL network simulator. It is used to study the dynamic nature of computer networks. There are many free and commercial simulators like GloMoSim, Openet, NetSim, QualNet. NS-2 refers to different network components such as routing, application etc. It is ongoing project of research and development. NS manual is also available for the guidance of users. It provides platform for the network protocols and helps to simulate their corresponding behaviour. NS-2 is a discrete platform where the events are scheduled with the scheduler. NS-2 takes input argument from users using executable command ns. Simulation trace file is created and is used for plotting graph and creating animation. C++ helps us to create the kernel of NS2.

NS-2 consists of two programming language C++ and Object-oriented Tool Command Language (OTcl). The requirement of two language is because C++ is fast to run but difficult to code and on the other hand OTcl is easy to code but very slow in running process. These two language when combined gives the platform for the simulation of ns-2. C++ helps us to modify the ns-2 modules and otcl helps us to run our events in the existing ns-2 modules.

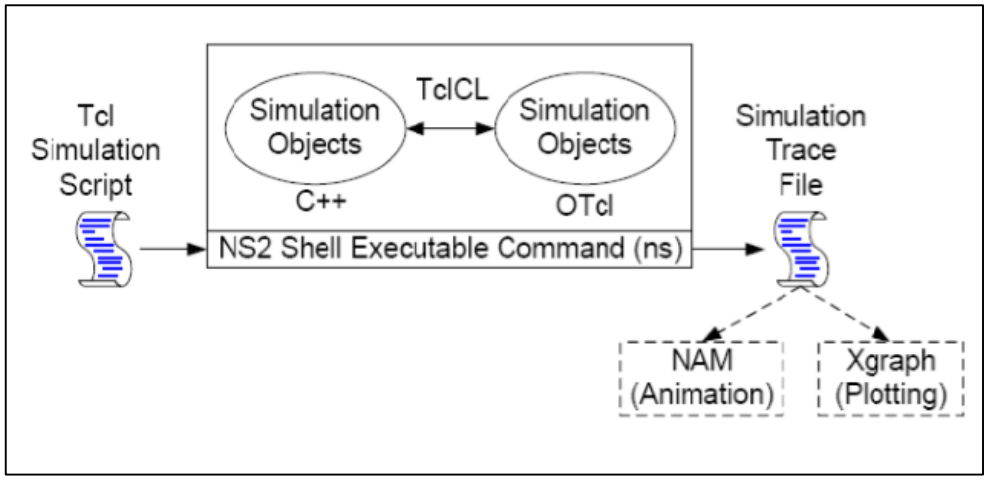

Figure 5.1 Layout of Network Simulator

The functioning of the components are discussed further.

- C++ : Internal mechanism (backend)
- OTcl : User interface (assemble , configure and schedule the objects) and front end language.
- TclCL: Linking C++ to OTcl

  NS-2 outputs 2 types of files after simulation. It can be either text based or animation based results. For analysing the result in graphically tools like NAM and XGraph are used.

5.1.2 Installation

NS-2 is an open and free simulation tool available on internet. UNIX or (Linux), Mac systems and windows are the various type of platforms which are used to run ns-2. NS-2 source codes are available in two forms of packages i.e. either all-in-one suite or component-wise. The main requirements of all-in-one suite are:-

- NS release 2.30
- Tcl/Tk release 8.4.13
- OTcl release 1.12,
- And TclCL release 1.18

Some of the optional requirements are:

- NAM (animation tool)
- Zlib version (library for NAM)

- Xgraph version (data plotter)

5.1.3 NS-2 includes 3 main steps:

- Design and Implementation: Firstly the user discover the purpose of simulation, assumption and the kind of results expected by the user from the simulation.
- Simulation: It includes two phase configuration and running. In configuration phase, the events are scheduled for the certain interval of time and network components are generated like UDP/TCP for making a network. In second phase, execution of events are done according to the simulation clock and configuration.
- Result compilation: This phase is mainly the debugging process. It includes evaluation of the performance.

5.2 Tool Command Language (Tcl)

It is the core language for NS-2. It act as an interpreter programming language developed by John Ouster at the University of California [38]. TCL is available in free and convenient to use**.** It is the scripting language. It uses different type of commands.

5.3 Object Oriented Tool Command Language (OTcl)

It helps us to specify the protocol and different network topologies. It is the programming language to configure the programs for network. Gedit in linux is used to write otcl script. It coordinates with the existing ns-2 modules.

5.4 Network Animator (NAM)

It is the visualization tool. It began in 1990. It is used for tracing the packets in the network and provide very useful information regarding the number of packets dropped by the malicious node or for visualizing the node movement. The command used to start the NAM is:

'nam < nam-file >' which is the name of the nam file created by ns-2. After the creation of nam file, it can be executed form the command prompt using this command:

>> nam filename.nam

The below screenshot in Fig 5.2 shows the functionality of the nam window. Many features are accessible in NAM like

- Animating coloured packet flows,
- dragging and dropping nodes (positioning),
- labelling nodes at a specified instant,
- Shaping the nodes,
- Colouring a specific link, and
- Monitoring a queue.

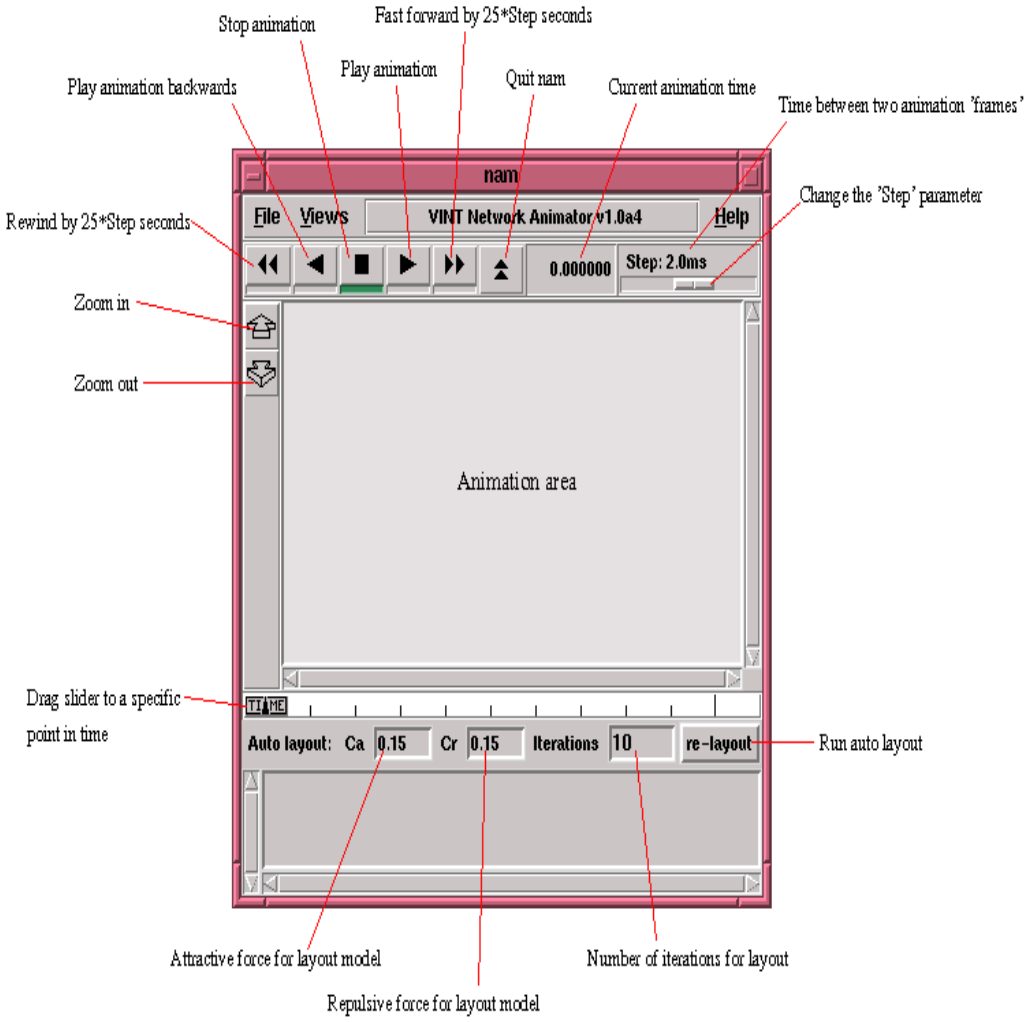

Figure 5.2 Display of Network animator.

5.5. Trace file

The functionality of trace file is to cover the data of overall network. The extension used for trace file is .tr and Otcl script is used for creating trace file. The simulation results are stored in trace file. The syntax for trace file is:

set nf [open simple.tr w] , where nf is used to handle the file and w means writing in a file [38].

$ns trace-all $nf , this command depicts to track every packet in the network.

The trace file is generated for wireless network in the Fig 5.3 below.

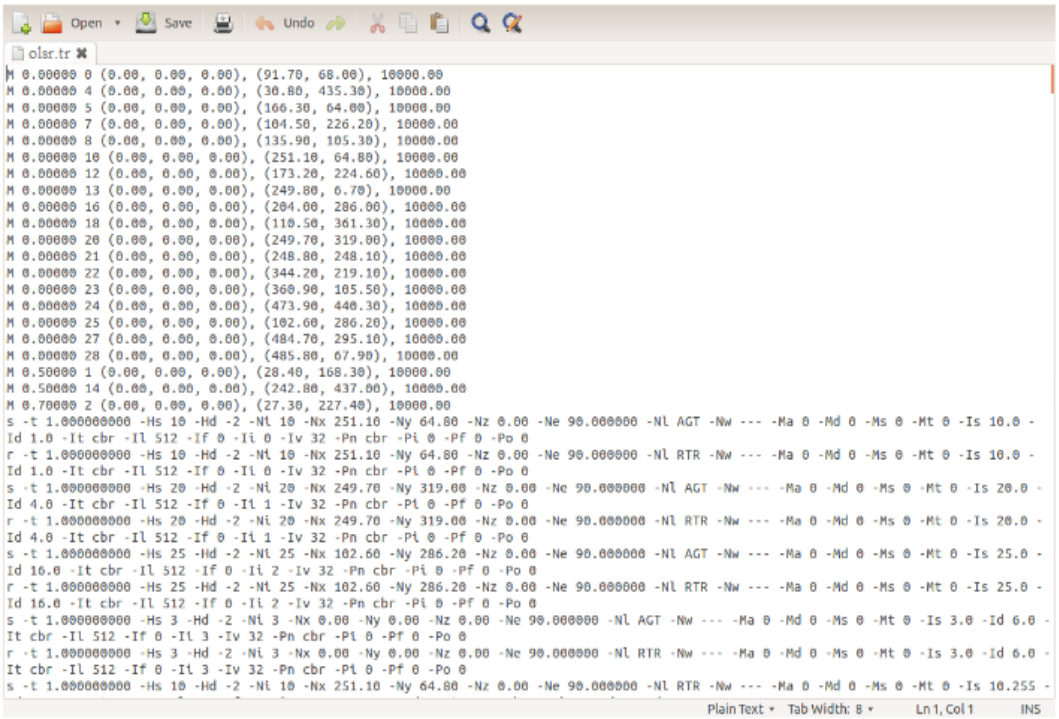

Fig 5.3 Trace file of OLSR

The trace file have ASCII code and includes 12 different fields as shown in below Fig 5.4.

Event	Time	From node	To node	Pkt type	Pkt size	Flags	Fid	Src addrs	Dst addrs	Seq num	Pkt id

Fig 5.4 Fields of Trace File.

The description of the various fields are below:

1.Event identifier: It tells the type of event and created by five fields which are +,- ,r, c and d respectively for queuing , **dequeuing**, receiving ,collision in the mac layer, dropped packets.

2. Time: It is the second field and tells the time at which the packet is occurred.

-Source and Destination node: These fields are the input/output id of the tracing object at which the events occurs.

3. Packet name: It tells the type of the packet like cbr (continuous bit rate) or tcp (transmission control protocol).

4. Packet size: The next field tells size of the packet in bytes.

5. Flags: The field stores the 7 digit flags.

6. Flow id: It is the flow identity of IPv6.

7. Source and Destination address: This field is in the form of node port.

8. Sequence number: It is the packet sequence number of network layer protocol. For the purpose of analysis it keeps track of the UDP.

9. Packet Unique id: It is the last field

Simulation results are stored into trace file (*.tr). Trace Graph was used to analyse the trace file [39].

Chapter 6

Results, Performance Evaluation & Analysis

In this chapter we obtained and evaluated the results done by simulation. The code was executed in TCL scripts having the extension .tr.

6.1 Simulation Setup

This section reports the performance of S-OLSR protocol on the basis of different parameters which shown in Table 6.1. The implementation is conducted with network simulator. In our simulation, we generated 48 wireless node including one attacker, one target node and one CBR source in a transmission area of 1000 meters by 1000 meters area. In our study each node follows random way point model which means mobility given to each node and repeated this process for several time. We run assessment for 50 seconds.

Simulator	NS-2 (version 2.35)
Routing Protocol	OLSR
Simulation time	50 seconds
Link bandwidth	2 Mbps
Traffic type	CBR
Packet rate	4pkt/s
Movement Model	Random way point
Packet size	512 bytes
Number of nodes	48
Number of attackers	1
Number of connections	1

Table 6.1 Simulator Parameters

The screenshot of node creation is shown in Fig 6.1.

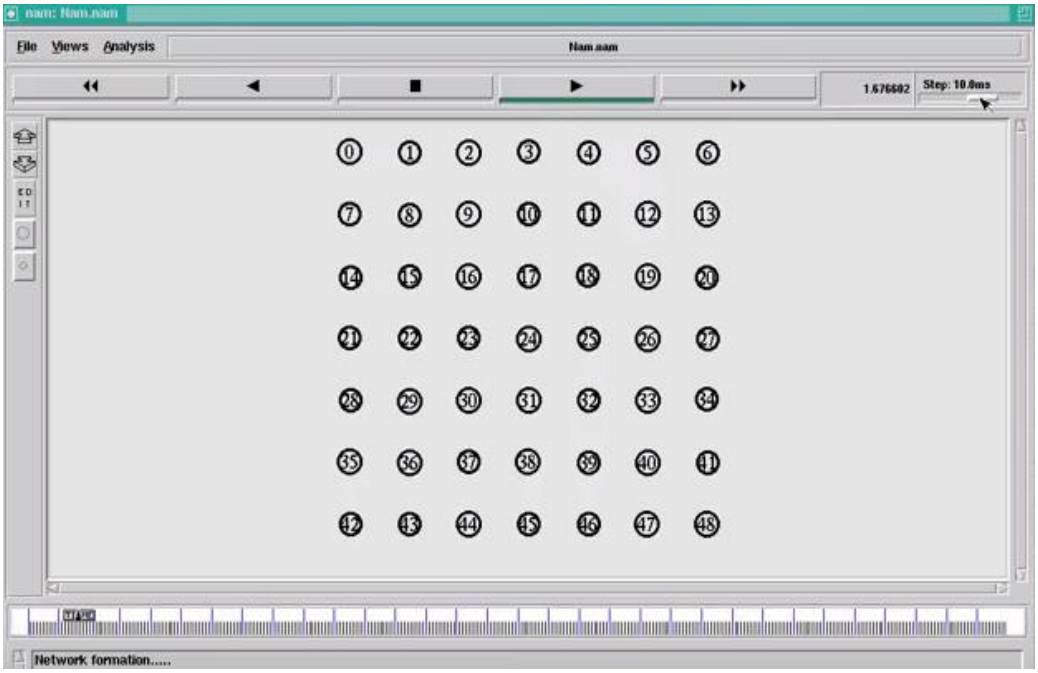

Fig 6.1 Node creation in NAM.

6.2 Link Spoofing Attack

In my work mainly focus on the mitigation of the link spoofing attack. In our simulation the data packets are sent from node 3 (source) to node 32 (destination) with the help of intermediate nodes 10, 17, 24. The node 17 acts as misbehaviour node. Link spoofing attack advertise that it has a fake link with next node and forces other node to select it as a MPR. The attacker dropped 93 packets out of 100. The output of the trace file is shown in Fig 6.2 and the network topology is in Fig 6.3.

```
-----------------------------------------------------------------
Time  Attacker-Id  Detected-Id    PACKET-DROPPED    PACKET-SENDED
-----------------------------------------------------------------
24.989999998   17        3    93    100
```

Fig 6.2 Output of trace file in link spoofing attack

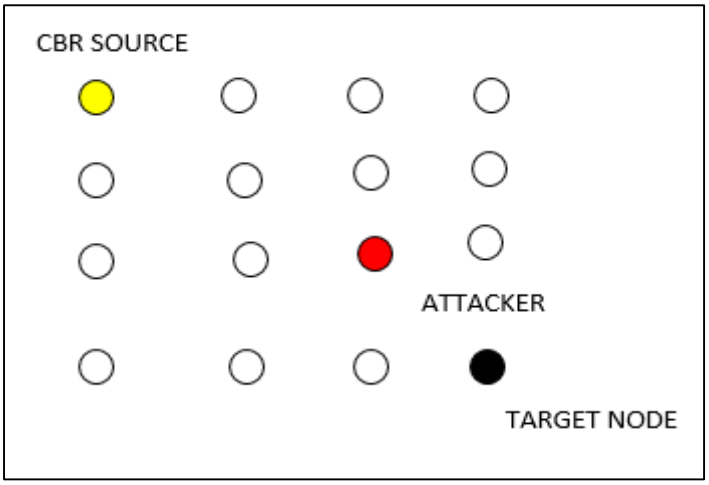

Fig 6.3 Example of network topology

Fig 6.4 Attacker node identification process

6.3 Working of the protocol

In Secure-OLSR the nodes broadcast Hello messages to the next nodes for the detection of the neighbor node. It is done periodically so that to get the latest update of the topology. Hello message is received by only 1-hop neighbour and not forwarded further. The main objective of the hello message is the neighboring sensing. The screenshot of the hello message broadcasted by the nodes are shown Fig 6.5

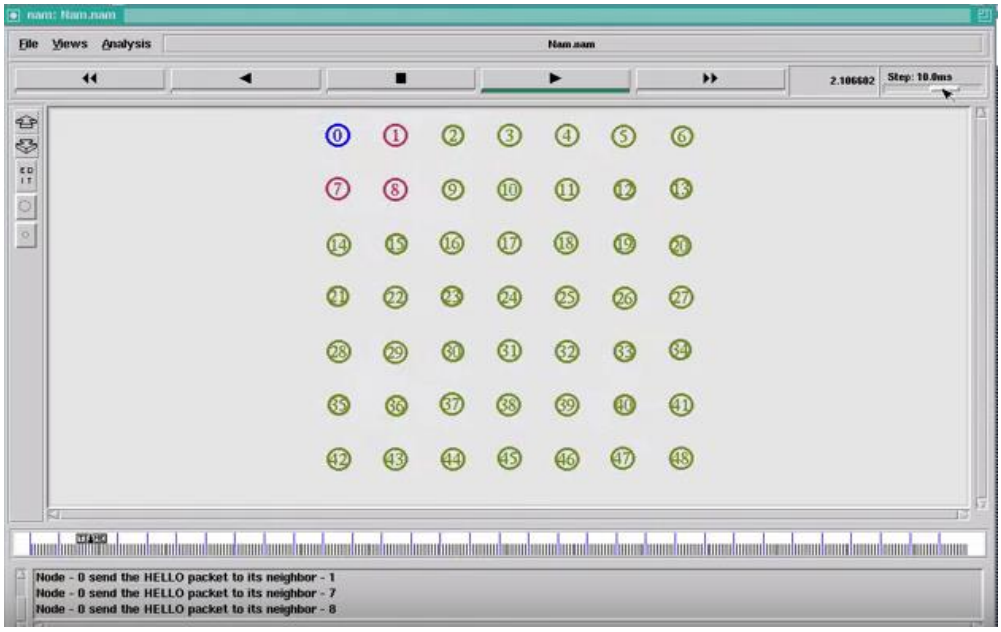

Fig 6.5 Broadcasting of hello packet.

6.3.1 Transmission Range

The transmission range of the node is denoted by circle. If receiver and sender node reside in the same range, then data packets are sent. If they don't reside or come in one another range then data packets are lost. The default range of transmission is 250m. The range can be obtained by setting the value receiving threshold (RXThresh_) in the coding. The screenshot of the transmission range is shown below in Fig 6.6.

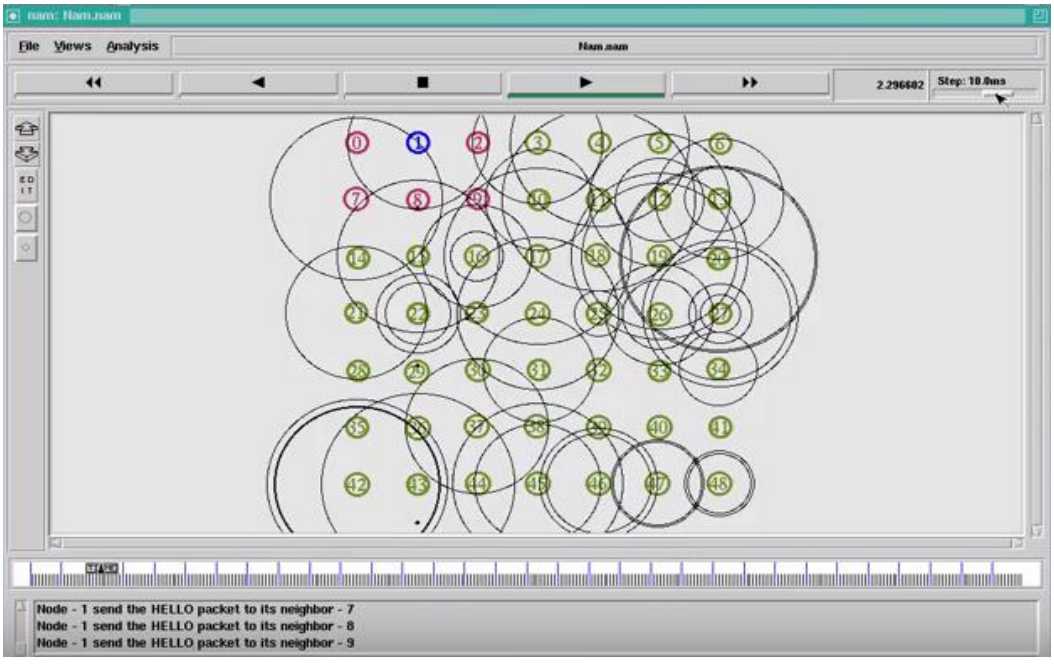

Fig 6.6 Model of Transmission Range

6.3.2 Internal Data structure of nodes

The Fig 6.7 is the sample code for printing and tracing the routing table, mpr set, 2 hop neighbour etc.

$ns_ at 5.0 "[$node_(0) agent 255] print_rtable"

$ns_ at 10.0 "[$node_(0) agent 255] print_linkset"

$ns_ at 15.0 "[$node_(0) agent 255] print_nbset"

$ns_ at 20.0 "[$node_(0) agent 255] print_nb2hopset"

$ns_ at 25.0 "[$node_(0) agent 255] print_mprset"

$ns_ at 30.0 "[$node_(0) agent 255] print_mprselset"

$ns_ at 35.0 "[$node_(0) agent 255] print_topologyset"

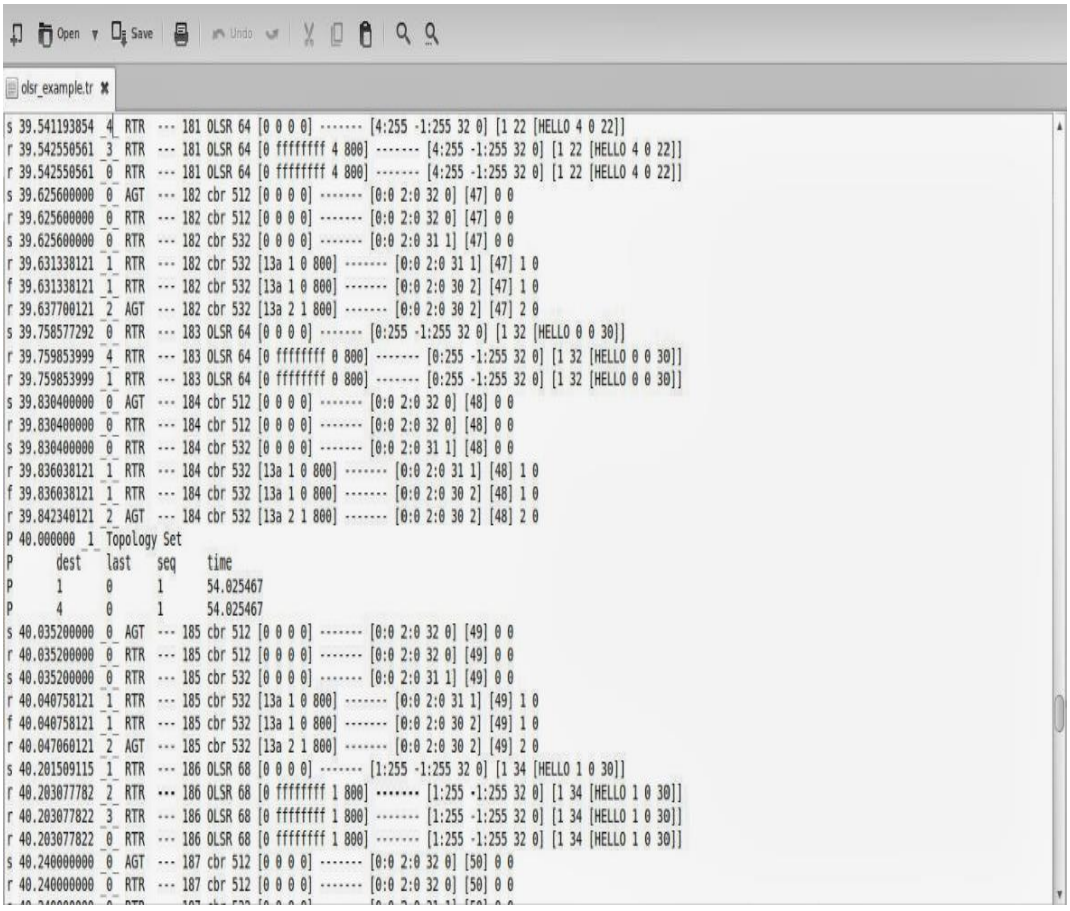

Fig 6.7 Output of the trace file for node 0.

```
P 10.000000_0_Routing Table
P       dest next iface dist
P        0    1    0     1
P        7    7    0     1
P        8    8    0     1
P        2    2    0     2
```

Fig 6.8 Screenshot of r_table.

```
P 15.000000_0_Link Set
P localnb   sym    asym    lost        time
P 0 1  20.563653  20.563653  0.000000 26.563653
P 0 7  20.457948  20.457948  0.000000 26.457948
P 0 8  20.511131  20.511131  0.000000 26.511131
```

Fig 6.9 Screenshot of link_set

```
P 20.000000 _0_ Neighbor Set
P       nb      status  willingness
P       1       1       3
P       7       1       3
P       8       1       3
```

Fig 6.10 Screenshot of neighbor_set

```
P 25.000000 _0_ Neighbor2hop Set
P       nb      nb2hop  time
P       0       4       29.878606
P       2       4       30.756880
```

Fig 6.11 Screenshot of 2hop_set

```
P 30.000000 _0_ MPR Set
P       nb
P       1
```

Fig 6.12 Screenshot of mpr_set

```
P 35.000000 _0_ MPR Selector Set
P       nb       time
P       7        40.819322
```

Fig 6.13 Screenshot of mprselector_set

6.3.3 Route Discovery

In OLSR the topology control packet is forwarded by MPR nodes. The route discovery process is done by these packets. They give us the information like one hop neighbor, 2- hop neighbor and helps in routing calculation. The screenshot below shown in Fig 6.14 is the functioning of the route_discovery by nodes.

Fig 6.14 Route discovery process

6.4 Performance Evaluation

In analysing the simulation, we have taken a single CBR connection which is farther from source by two hops. All node varies with arbitrary speed. The pause time is fixed to 0. The variation in the speed of each node from 0m/s to 12m/s in 3m/s increments and observe the PDR of each scenario. The performance metrics taken are packet delivery ratio and average throughput.

6.4.1 Packet Delivery Ratio (PDR)

The packet delivery ratio (PDR) is based on the count of received and generated packets. The formula used for evaluating PDR is

packet_delivery_ratio = received_packets/generated_packets*100.

By implementing our protocol on ns2 we got 98.9011% pdr value as generated packets are 819 and received packets are 810.

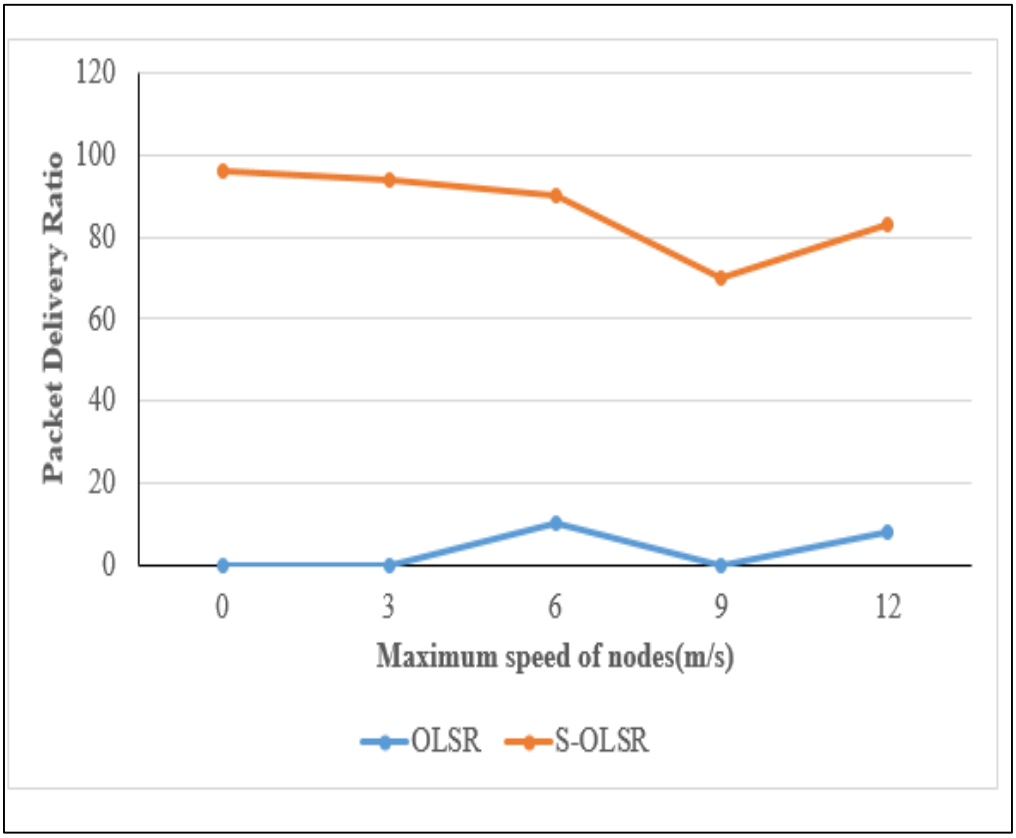

Fig 6.15 Result of Packet Delivery Ratio

The experimental work is shown in Fig 6. It can be seen PDR is zero as no packet is transmitted to target node in current OLSR under link spoofing attack but in our approach the values of packet received increases, hence PDR is much higher. Our approach provide protection from link spoofing attack.

6.4.2 Throughput

It is the count of data reached fully to the destination in a unit time. It is denoted in bps. The formula used to calculate it is throughput

t= received_data*8/ DataTransmissionPeriod.

The result is 3.45522MB/s.

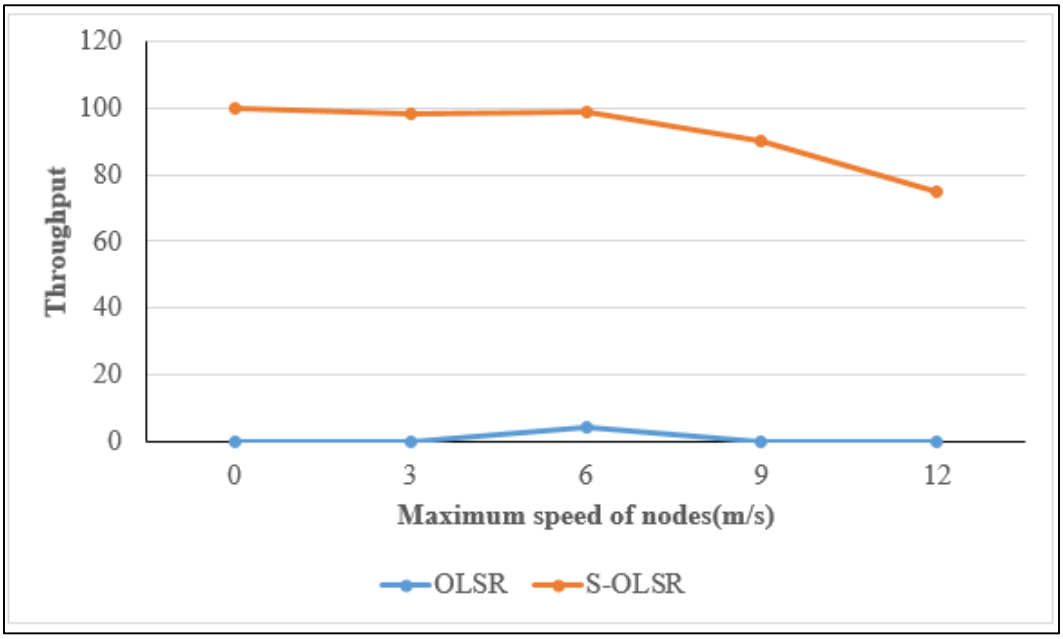

Fig 6.16 Result of Throughput.

Chapter 7

Conclusion and Future Scope

Security is the primary concern of ad hoc networks. Malicious nodes and attackers are always prepared to interrupt the network. Optimized Link State Routing is in trends now days. Therefore it is vulnerable to many different kind of attacks.

In this thesis work, we have presented Secure-OLSR mechanism. It has been effective to mitigate link spoofing attack. Our approach is basically on exchanging 2-hop_*ACK* and 2-HOP_*req* control packets. The main comfort of our mechanism is that it do not need complete knowledge of topology. There is no need for hardware specification also. For validating, our mechanism we have done implementation on network simulator.

With the help of NAM and trace graph we were able to get the effective results. The simulation results show the effectiveness of our mechanism over the link spoofing attack.

References Annexure I

[1] Jacquet, Philippe, et al. "Optimized link state routing protocol for ad hoc networks." *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International*. IEEE, 2001.

[2] Royer, Elizabeth M., and Chai-Keong Toh. "A review of current routing protocols for ad hoc mobile wireless networks." *Personal Communications, IEEE* 6.2 (1999): 46-55.

[3] Roy, Sudipta, et al. "International Journal of Advanced Research in Computer Science and Software Engineering." *International Journal* 3.6 (2013).

[4] Mohseni, Shima, et al. "Comparative review study of reactive and proactive routing protocols in MANETs." *Digital ecosystems and technologies (DEST), 2010 4th IEEE international conference on*. IEEE, 2010.

[5] Gagandeep, Aashima, and Pawan Kumar. "Analysis of different security attacks in MANETs on protocol stack A-review." *International Journal of Engineering and Advanced Technology* 1.5 (2012): 269-275.

[6] Kaur, Robinpreet, and Mritunjay Kumar Rai. "A Novel Review on Routing Protocols in MANETs." *Undergraduate Academic Research Journal (UARJ), ISSN* 2278 (2012): 1129.

[7] Adjih, C., Clausen, T., Jacquet, P., Laouiti, A., Muhlethaler, P., & Raffo, D. (2003, June). Securing the OLSR protocol. In *Proceedings of Med-Hoc-Net* (pp. 25-27)

[8] Srivastava, Anurag, et al. "Survey and overview of Mobile Ad-Hoc Network routing protocols." *Advances in Engineering and Technology Research (ICAETR), 2014 International Conference on*. IEEE, 2014.

[9] Patel, Daxesh N., et al. "A survey of reactive routing protocols in MANET."*Information Communication and Embedded Systems (ICICES), 2014 International Conference on*. IEEE, 2014.

[10] Mistry, Hetal P., and Nital H. Mistry. "A survey: Use of ACO on AODV & DSR routing protocols in MANET." *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on*. IEEE, 2015.

[11] Kanakaris, Venetis, David Ndzi, and Djamel Azzi. "Ad-hoc networks energy consumption: a review of the ad-hoc routing protocols." *Journal of Engineering Science and Technology Review (JESTR)* 3.1 (2010): 162-167.

[12] Von Mulert, Jan, Ian Welch, and Winston KG Seah. "Security threats and solutions in MANETs: A case study using AODV and SAODV." *Journal of network and computer applications* 35.4 (2012): 1249-1259.

[13] Nguyen, Dang Quan, and Pascale Minet. *Analysis of Multipoint relays Selection in the OLSR Routing Protocol with and without QoS Support*. Diss. INRIA, 2006.

[14] Raffo, Daniele, et al. "An advanced signature system for OLSR."*Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2004.

[15] Rahman, Abdul Hadi Abd, and Zuriati Ahmad Zukarnain. "Performance comparison of AODV, DSDV and I-DSDV routing protocols in mobile ad hoc networks." *European Journal of Scientific Research* 31.4 (2009): 566-576.

[16] Adjih, Cedric, et al. "Fish eye OLSR scaling properties." *Communications and Networks, Journal of* 6.4 (2004): 343-351.

[17] Haas, Zygmunt J., Marc R. Pearlman, and Prince Samar. "The zone routing protocol (ZRP) for ad hoc networks." (2002).

[18] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." *Human-centric Computing and Information Sciences* 1.1 (2011): 1-16.

[19] Kannhavong, Bounpadith, et al. "Analysis of the node isolation attack against OLSR-based mobile ad hoc networks." *Computer Networks, 2006 International Symposium on*. IEEE, 2006.

[20] Balakrishnan, Venkatesan, and Vijay Varadharajan. "Packet drop attack: A serious threat to operational mobile ad hoc networks." *Proceedings of the International Conference on Networks and Communication Systems (NCS 2005), Krabi*. 2005.

[21] Sen, Jaydip, et al. "A mechanism for detection of gray hole attack in mobile Ad Hoc networks." *Information, Communications & Signal Processing, 2007 6th International Conference on*. IEEE, 2007.

[22] Kannhavong, Bounpadith, Hiroki Nakayama, and Abbas Jamalipour. "SA-OLSR: Security aware optimized link state routing for mobile ad hoc networks." *Communications, 2008. ICC'08. IEEE International Conference on*. IEEE, 2008.

[23] Raffo, Daniele, et al. "An advanced signature system for OLSR."*Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2004.

[24] Djahel, Soufine, Farid Nait-Abdesselam, and Ashfaq Khokhar. "An acknowledgment-based scheme to defend against cooperative black hole attacks in optimized link state routing protocol." *Communications, 2008. ICC'08. IEEE International Conference on*. IEEE, 2008.

[25] Zhao, Ziming, et al. "Risk-aware mitigation for MANET routing attacks."*Dependable and Secure Computing, IEEE Transactions on* 9.2 (2012): 250-260.

[26] García Villalba, L. Javier, et al. "Secure extension to the optimised link state routing protocol." *Information Security, IET* 5.3 (2011): 163-169.

[27] Shivanakar, Balaji S., and Sandeep A. Thorat. "Addressing node isolation attack in OLSR protocol." *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*. IEEE, 2015.

[28] Wang, Maoyu, et al. "An effective intrusion detection approach for OLSR MANET protocol." *Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNP Workshop on*. IEEE, 2005.

[29] Vidhya, K. Urmila, and M. Mohana Priya. "A novel technique for defending routing attacks in OLSR MANET." *IEEE International Conference on Computational Intelligence and Computing Research*. 2010.

[30] Von Mulert, Jan, Ian Welch, and Winston KG Seah. "Security threats and solutions in MANETs: A case study using AODV and SAODV." *Journal of network and computer applications* 35.4 (2012): 1249-1259.

[31] Jeon, Yuseok, et al. "LT-OLSR: Attack-tolerant OLSR against link spoofing."*Local Computer Networks (LCN), 2012 IEEE 37th Conference on*. IEEE, 2012.

[32] Vilela, João P., and João Barros. "A cooperative security scheme for optimized link state routing in mobile ad-hoc networks." *Proceedings of the 15th IST Mobile and Wireless Communications Summit, Mykonos, Greece*(2006).

[33] Song, Ronggong, and C. Mason Peter. "ROLSR: A robust optimized link state routing protocol for military ad-hoc networks." *MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010*. IEEE, 2010.

[34] Wang, Anbao, and Bin Zhu. "Improving MPR selection algorithm in OLSR protocol based on node localization technology." *Journal of Networks* 9.7 (2014): 1674-1681.

[35] Joshi, Radhika D., and Priti P. Rege. "Implementation and analytical modelling of modified optimised link state routing protocol for network lifetime improvement." *Communications, IET* 6.10 (2012): 1270-1277.

[36] Marc Greis. Ns Tutorial. http://www.isi.edu/nsnam/ns/tutorial/index.html

[37] S. McCanne and S. Floyd. Network Simulator. http://www.isi.edu/nsnam/ns/

[38] TCL Tutorial. http://www.tcl.tk/man/tcl8.5/tutorial/tcltutorial.html

[39] Tracegraph http://www.tracegraph.com/download.html

Abbreviations Annexure II

ACK	Acknowledgement
AODV	Ad hoc On-Demand Distance Vector Routing
CSS-OLSR	Cooperative Security Scheme
CBR	Constant Bit Rate
CPM	Complete Path Message
DSR	Dynamic Source Routing
DSDV	Destination Sequence Distance Vector
DAG	Directed Acyclic Graph
DOS	Denial of Service
LT-OLSR	Attack Tolerant OLSR
MPR	Multi Point Relay
MSN	Message Sequence Number
MANET	Mobile Ad Hoc network
MAC	Medium Access Control
NS	Network Simulator
NAM	Network Animator
OLSR	Optimized Link State Routing
OTCL	Object-oriented Tool Command Language
R-OLSR	Robust OLSR
RREQ	Route Request Packet
SA-OLSR	Security Aware Optimized Link State Routing
TCL	Tool Command Language
TCP	Transmission Control Protocol
TC	Topology Control
UDP	User Datagram Protocol
ZRP	Zone Routing Protocol

List of Publications Annexure III

Accepted

- **Thirteenth International Conference on Wireless and Optical Communications Networks WOCN2016**

Link

- **https://youtu.be/vjBlEzy_Nf8**

.